

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



~~2766~~ #2  
2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): DIRK ROSENAU ET AL—

SERIAL NO.: 09/593,406 —

Group Art Unit: 2766

FILED: June 14, 2000 —

TITLE: "ARRANGEMENT AND METHOD FOR GENERATING A—  
SECURITY IMPRINT"—

Assistant Commissioner of Patents

Washington, D.C. 20231

**SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT**

SIR:

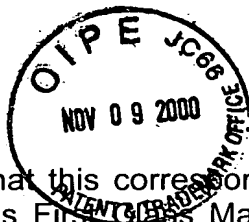
Applicants herewith submit a Certified Copy of German Application No. 199 28 058.4, filed in the German Patent and Trademark Office on June 15, 1999, on which Applicants base their claim for convention priority under 35 U.S.C. §119.

Respectfully submitted,

 (Reg. #28,982)

Steven H. Noll  
SCHIFF HARDIN & WAITE  
Patent Department  
6600 Sears Tower  
Chicago, Illinois 60606  
Telephone: 312-258-5790  
Attorneys for Applicants

RECEIVED  
NOV 14 2000  
TC 2700 MAIL ROOM



I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner of Patents, Washington, D. C. 20231 on November 7, 2000.

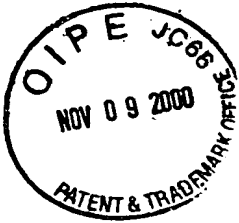
Steven H. Noll

Name of Applicants' Attorney

Signature

November 7, 2000

Date



## Bescheinigung

Die Francotyp-Postalia AG & Co in Birkenwerder/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Anordnung und Verfahren zur Generierung eines Sicherheitsabdruckes"

am 15. Juni 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol G 07 B 17/02 der Internationalen Patentklassifikation erhalten.

München, den 16. Mai 2000

**Deutsches Patent- und Markenamt**

**Der Präsident**

Im Auftrag

Aktenzeichen: 199 28 058.4

**Jerofsky**

Francotyp-Postalia AG & Co.  
Triftweg 21 - 26  
16547 Birkenwerder

15. Juni 1999

3160-DE

---

Anordnung und Verfahren zur Generierung eines Sicherheitsabdruckes

---

Beschreibung

Die Erfindung betrifft eine Anordnung zur Generierung eines Sicherheitsabdruckes mit einem Sicherheitsmodul, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art und für ein Verfahren zur Generierung eines Sicherheitsabdruckes, gemäß der im Oberbegriff des Anspruchs 12 angegebenen Art. Ein postalischer Sicherheitsmodul ist ein Teil einer Anordnung, die sich insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion eignet. Das Verfahren dient der Sicherung vor einer Manipulation mit nichtbezahlten Frankierungen auf Postgütern.

In EP 862 143 A2 wurde eine Frankiermaschine für die Erzeugung und Überprüfung eines Sicherheitsabdruckes vorgeschlagen. Ein Sicherheitsabdruck weist eine maschinenlesbare Markierung mit variablen Daten und einen Krypto- bzw. Authentisierungscode auf.

Zur Überprüfung des Sicherheitsabdruckes wird ein aus den variablen Daten gebildeter Krypto- bzw. Authentisierungscode mit dem aufgedruckten Krypto- bzw. Authentisierungscode verglichen. Die Frankiermaschine hat einen einzigen Mikroprozessor, der sowohl einen Kryptocode bzw.

einen DAC (DATA AUTHENTICATION CODE) zur Absicherung der Druckdaten, als auch das Druckbild selbst berechnet. Letzteres besteht aus festen Rahmenpixeldaten und den Fensterpixeldaten. Fensterpixeldaten sind variable und semivariable Druckdaten.

5 Dabei wurde vorgeschlagen, um die Rechenzeit optimal auszunutzen, die Druckdaten für den Krytocode bzw. einen DAC und diejenigen variablen Daten, die sich relativ häufig ändern, erst kurz vor dem Drucken in das berechnete Druckbild einzufügen. Bei Frankiermaschinen mit spaltenweisen Druck auf ein bewegtes Postgut, wobei die Druckzeile im Druckkopf orthogonal zur Transportrichtung des Briefes angeordnet ist, kann  
10 sich eine Möglichkeit ergeben, die vorgenannten variablen Daten direkt in das Druckregister der Drucksteuerung für den Druckkopf zu übertragen, wobei die Übertragung sequentiell mit den Rahmenpixeldaten erfolgt. Damit wird eine Möglichkeit geschaffen, erst spät fertigberechnete DAC-Druckdaten auch noch nachträglich während des Druckens einzubetten.  
15 Beispielsweise bei der Frankiermaschine T1000 der Anmelderin, welche nach einem Thermo-transferdruckverfahren arbeitet, ergibt sich bei Lauflängencodierung der Druckdaten, eine solche Möglichkeit unter der Voraussetzung, daß bereits einige der festen Rahmenpixeldaten und der zuvor eingebetteten Fensterpixeldaten bereits gedruckt werden, so daß  
20 die DAC-Druckdaten erst spät eingebettet können, weil das entsprechende Fenster erst später gedruckt werden muß. Wenn jedoch seitens eines Postbeförderers die Forderung besteht, das betreffende Fenster zuerst zu drucken, muß die Einbettung der Druckdaten im Vorab erfolgen. Wenn die  
25 Änderungen sich über mehrere Druckspalten erstrecken, wobei mehr als die Hälfte der Druckspalten des gesamten Druckbildes verändert werden müssen, resultiert daraus eine entsprechende Verlängerung der Rechenzeit. Dann ist aber vor jedem Frankierbildausdrucken eine Neuberechnung des Druckbildes mit anderen variablen Fensterdaten und mit  
30 neuen DAC-Druckdaten nötig. Der Durchsatz beim Frankieren wird bei solchen Druckbildern für einen Sicherheitsabdruck deutlich verringert.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Anordnung zu entwickeln, um den Durchsatz an Post beim Frankieren mit  
35 einem Sicherheitsabdruck zu erhöhen.

Bei Frankiermaschinen mit hohem Durchsatz (Systemtakt) ist eine Technik zu entwickeln, bei der nach jeder erfolgreichen Abrechnung der Fran-

kierabdruck durch einen Sicherheitscode signiert wird. Hierbei muß die Signatur schnell genug errechnet werden, um sie abhängig vom Systemtakt der Frankiermaschine schnell genug für die Druckbildberechnung zur Verfügung zu stellen. Auch wenn die Änderungen in den Druckdaten von  
5 Abdruck zu Abdruck maximal sind, soll dadurch der Durchsatz nicht verringert werden, daß ein Sicherheitsabdruck gedruckt wird.

Die Aufgabe wird mit den Merkmalen des Anspruchs 1 für eine Anordnung und mit den Merkmalen des Anspruchs 12 für ein Verfahren gelöst.

10 Eine Lösung des Problems wurde in der Durchführung von zwei zeitlich versetzten Berechnungen durch unterschiedliche Rechner gefunden. Die Berechnung des Sicherheitscodes wird erfindungsgemäß von einem separaten Sicherheitsmodul vorgenommen, während die Druckbilddaten-  
aufbereitung vom Frankiermaschinen-Prozessor vorgenommen wird.  
15 Durch geschicktes Verschachteln der beiden Aufgaben und spezielle Auswahl von Algorithmen und Datenstrukturen wird eine hohe System-  
taktleistung erzielt.

Das Sicherheitsmodul wird so implementiert, daß alle für den  
20 Sicherheitscode DAC benötigten Systemdaten über Nachrichten von der Frankiermaschine voreingestellt werden. Jede Nachricht, die solche Systemdaten verändert, startet sofort, sofern die neuen Systemdaten vom Sicherheitsmodul als gültig erkannt werden, eine Neuberechnung des Sicherheitscodes. Eine über eine separate Nachricht an das  
25 Sicherheitsmodul gemeldete Aufforderung zur Abrechnung startet die Abrechnung. Das Sicherheitsmodul sendet den Sicherheitscode an die Frankiermaschine FM, wobei letztere die Druckdatenaufbereitung und Berechnung des Druckbildes vornimmt. Für Massenfrankierungen mit hohem Systemtakt ergibt sich folgende zeitliche Verschachtelung der  
30 Operationen beider Datenverarbeitungseinheiten, die zu einer hohen Systemleistung führt. Die zeitliche Verschachtelung läßt sich nur durch folgende zwei Maßnahmen ermöglichen:

1. Zwei Verarbeitungseinheiten (FM / FPSM)
2. Vorberechnung des Sicherheitscodes aufgrund voreingestellter Werte

Das Verfahren findet beispielsweise in Frankiermaschinen Anwendung, für die besondere Sicherheitsforderungen bezüglich der Postregisterdaten und des Abdruckes gelten, da insbesondere die geldwerten Abrechnungsdaten unmanipulierbar sein müssen.

5

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

10

Figur 1a, Zeit/Steuerungsdiagramm für eine Frankiermaschine bekannter Art mit einem Mikroprozessor,

15

Figur 1b, Zeit/Steuerungsdiagramm für eine Frankiermaschine nach der Erfindung mit einem Mikroprozessor im Meter für die Druckaufgaben und einem Sicherheitsmodul für die Sicherheitsaufgaben,

20

Figur 2, Blockschaltbild einer Frankiermaschine mit Sicherheitsmodul,

Figur 3, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 4, Darstellung eines Sicherheitsabdrucks,

25

Figur 5, Blockschaltbild des Sicherheitsmoduls,

Figur 6, Flußdiagramm für das Erzeugen von Sicherheitsabdrucken beim Frankieren.

30

In der Figur 1a ist ein Zeit/Steuerungsdiagramm für eine Frankiermaschine dargestellt, die in bekannter Art mit einem Mikroprozessor ausgestattet ist, der für das Erzeugen von Sicherheitsabdrucken beim Frankieren folgende Schritte ausführt:

35

- Eingaberoutine 401, um den Portowert einzustellen,
- Sensorroutine 402, um die Briefanlage festzustellen, mit



- Subroutine 406-411 zur DAC-Berechnung,
- Aufforderungsroutine 403 zum Abrechnen, mit
- Subroutine 412, 413 zum Abrechnen und mit
- Subroutine zum DAC bereitstellen,
- 5 - Berechnungsroutine 404 für das Druckbild sowie
- Druckroutine 405.

Aufgrund der sequentiellen Verarbeitung der Daten bei der Durchführung der einzelnen Routinen und Subroutinen wird eine Datenverarbeitungszeitdauer  $T_{alt}$  je Frankierung mit einem Sicherheitsabdruck benötigt.

Das erfindungsgemäße – in der Figur 1b gezeigte - Zeit/Steuerungsdiagramm für eine Frankiermaschine benötigt eine Datenverarbeitungszeitdauer  $T_{neu}$  je Frankierung mit einem Sicherheitsabdruck, welche

15 kürzer ist, als die alte Datenverarbeitungszeitdauer  $T_{alt}$  je Frankierung. Das ist nur möglich, weil bei der Erfindung eine Aufgabenteilung für zwei Datenverarbeitungseinheiten stattfindet, wobei ein Mikroprozessor im Meter für die Druckaufgaben und ein Sicherheitsmodul für die Sicherheitsaufgaben vorgesehen ist.

20 Die Druckaufgaben umfassen eine Eingaberoutine 401, um den Portowert einzustellen, eine Sensorroutine 402, um die Briefanlage festzustellen, eine Aufforderungsroutine 403 zum Abrechnen, eine Berechnungsroutine 404 für das Druckbild sowie eine Druckroutine 405.

25 Die Sicherheitsaufgaben umfassen eine Subroutine 406-411 zur DAC-Berechnung, eine Subroutine 412, 413 zum Abrechnen und eine Subroutine zum DAC bereitstellen.

Die Berechnungsroutine 404 für das Druckbild ist besonders aufwendig

30 für einen Sicherheitsabdruck, deshalb wird mit dem Druckbildaufbau schon vor dem Ende der Abrechnung begonnen. Außerdem führt der Mikroprozessor im Meter die Druckroutine 405 durch, während der Sicherheitsmodul bereits den Sicherheitscode das nächste Druckbild berechnet, sobald das Anlegen eines weiteren Briefes am Eingang des

35 Transportweges von einem Briefsensor erfaßt wird.

Das ist besonders bei Massenfrankierungen von Poststücken, insbesondere von Briefen, mit dem gleichen Portowert sinnvoll. Das Anlegen eines weiteren Briefes, welches am Eingang des Transportweges von einem Briefsensor erfaßt wird, löst einen Interrupt für den Mikroprozessor im Meter aus, welcher die Briefanlage an das Sicherheitsmodul weitermeldet und dann die begonnenen Berechnungen zum Druckbildaufbau fortsetzt. In dem Patent US 5,710,721 wurde unter dem Titel: INTERNAL POSTAGE METER MACHINE INTERFACE CIRCUIT prinzipiell beschrieben, wie bei einem Sensorsignal ein Interrupt für den Mikroprozessor ausgelöst wird und wie die Drucksteuerung arbeitet. Erfindungsgemäß arbeitet der Mikroprozessor noch am Druckbildaufbau (schritt 404) oder ist mit der Durchführung der Druckroutine (Schritt 405) beschäftigt, während die Weitermeldung 412 einer weiteren Briefanlage an das Sicherheitsmodul SM erfolgt, woraufhin letzteres bereits weiterer Berechnungen 316-321 für ein nächstes Poststück (Brief) durchführt. Sobald der Mikroprozessor mit der Durchführung der Druckroutine (Schritt 405) fertig ist, ergeht eine Aufforderung an das Sicherheitsmodul, eine Abrechnung durchzuführen. Das Sicherheitsmodul SM führt nun die Abrechnung (Schritte 322, 323) durch und sendet (Schritt 324) den Sicherheitscode DAC an den Mikroprozessor 91 des Meters, welches nun in der Lage ist den Druckbildaufbau für das weitere Druckbild zuende zu führen (Schritt 414).

Die Figur 2 zeigt ein Blockschaltbild einer Frankiermaschine. Die Steuereinrichtung 1 weist ein mit einem Mikroprozessor 91 mit zugehörigen Speichern 92, 93, 94, 95 ausgestattetes Motherboard 9 auf.

Der Programmspeicher 92 enthält ein Betriebsprogramm mindestens zum Drucken und wenigstens sicherheitsrelevante Bestandteile des Programms für eine vorbestimmte Format-Änderung eines Teils der Nutzdaten.

Der Arbeitsspeicher RAM 93 dient zur flüchtigen Zwischenspeicherung von Zwischenergebnissen. Der nichtflüchtige Speicher NVM 94 dient zur nichtflüchtigen Zwischenspeicherung von Daten, beispielsweise von statistischen Daten, die nach Kostenstellen geordnet sind. Der

Kalender/Uhrenbaustein 95 enthält ebenfalls adressierbare aber nichtflüchtige Speicherbereiche zur nichtflüchtigen Zwischenspeicherung von Zwischenergebnissen oder auch bekannten Programmteilen. Es ist vorgesehen, daß die Steuereinrichtung 1 mit einer Chipkarten-Schreib/Leseeinheit 70 verbunden ist, wobei der Mikroprozessor 91 der Steuereinrichtung 1 beispielsweise dazu programmiert ist, die Nutzdaten N aus dem Speicherbereich einer Chipkarte 49 zu deren Anwendung in entsprechende Speicherbereiche der Frankiermaschine zu laden. Eine in einen Einsteckschlitz 72 der Chipkarten-Schreib/Leseeinheit 70 eingesteckte erste Chipkarte 49 gestattet ein Nachladen eines Datensatzes in die Frankiermaschine für mindestens eine Anwendung. Die Chipkarte 49 enthält beispielsweise die Portogebühren für alle üblichen Postbefördererleistungen entsprechend des Tarifs der Postbehörde und ein Postbefördererkennzeichen, um mit der Frankiermaschine ein Stempelbild zugenerieren und entsprechend des Tarifs der Postbehörde die Poststücke freizustempeln.

Die Steuereinrichtung 1 bildet das eigentliche Meter mit den Mitteln 91 bis 95 der vorgenannten Hauptplatine 9 und umfaßt auch eine Tastatur 88, eine Anzeigeeinheit 89 sowie einen anwendungsspezifischen Schaltkreis ASIC 90 und das Interface 8 für das postalische Sicherheitsmodul PSM 100. Das Sicherheitsmodul PSM 100 ist über einen Steuerbus mit dem vorgenannten ASIC 90 und dem Mikroprozessor 91 sowie über den parallelen µC-Bus mindestens mit den Mitteln 91 bis 95 der Hauptplatine 9 und der mit Anzeigeeinheit 89 verbunden. Der Steuerbus führt Leitungen für die Signale CE, RD und WR zwischen dem Sicherheitsmodul PSM 100 und dem vorgenannten ASIC 90. Der Mikroprozessor 91 weist vorzugsweise einen Pin für ein vom Sicherheitsmodul PSM 100 abgegebenes Interruptsignal i, weitere Anschlüsse für die Tastatur 88, eine serielle Schnittstelle SI-1 für den Anschluß der Chipkarten-Schreib/Lese-Einheit 70 und eine serielle Schnittstelle SI-2 für den optionalen Anschluß eines MODEMs auf. Mittels des MODEMs kann beispielsweise das im nichtflüchtigen Speicher des postalischen Sicherheitsmittels PSM 100 gespeicherte Guthaben erhöht werden.

Das postalische Sicherheitsmittel PSM 100 wird von einem gesicherten Gehäuse umschlossen. Vor jedem Frankierabdruck wird im postalischen Sicherheitsmodul PSM 100 eine hardwaremäßige Abrechnung durchgeführt. Die Abrechnung erfolgt unabhängig von Kostenstellen.

Es ist vorgesehen, daß der ASIC 90 eine serielle Schnittstellenschaltung 98 zu einem im Poststrom vorschalteten Gerät, eine serielle Schnittstellenschaltung 96 zu den Sensoren und Aktoren der Druckeinrichtung 2, eine serielle Schnittstellenschaltung 97 zur Drucksteuerelektronik 16 für den Druckkopf 4 und eine serielle Schnittstellenschaltung 99 zu einem der Druckeinrichtung 20 im Poststrom nachgeschalteten Gerät aufweist. Der DE 197 11 997 ist eine Ausführungsvariante für die Peripherieschnittstelle entnehmbar, welche für mehrere Peripheriegeräte (Stationen) geeignet ist. Sie trägt den Titel:  
Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

Die Schnittstellenschaltung 96 gekoppelt mit der in der Maschinenbasis befindlichen Schnittstellenschaltung 14 stellt mindestens eine Verbindung zu den Sensoren 6, 7, 17 und zu den Aktoren, beispielsweise zum Antriebsmotor 15 für die Walze 11 und zu einer Reinigungs- und Dichtstation RDS 40 für den Tintenstrahldruckkopf 4, sowie zum Labelgeber 50 in der Maschinenbasis her. Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf 4 und der RDS 40 sind der DE 197 26 642 C2 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

Einer der in der Führungsplatte 20 angeordneten Sensoren 7, 17 ist der Sensor 17 und dient zur Vorbereitung der Druckauslösung beim Brieftransport. Der Sensor 7 dient zur Briefanfangserkennung zwecks Druckauslösung beim Brieftransport. Die Transporteinrichtung besteht aus einem Transportband 10 und zwei Walzen 11, 11'. Eine der Walzen ist die mit einem Motor 15 ausgestattete Antriebswalze 11, eine andere ist die mitlaufende Spannwalze 11'. Vorzugsweise ist die Antriebswalze 11 als Zahnwalze ausgeführt, entsprechend ist auch das Transportband 10 als Zahnriemen ausgeführt, was die eindeutige Kraftübertragung sichert. Ein Encoder 5, 6 ist mit einer der Walzen 11, 11' gekoppelt. Vorzugsweise sitzt die Antriebswalze 11 mit einem Inkrementalgeber 5 fest auf einer Achse. Der Inkrementalgeber 5 ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke 6 zusammen wirkt, und gibt über die Leitung 19 ein Encodersignal an das Motherboard 9 ab.

Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der Druckkopf für einen rein elektronischen Druck ansteuerbar ist. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur 88  
5 oder bei Bedarf per Chipkarte eingegeben und im Speicher NVM 94 nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenenfalls weiteren Druckbildern für Werbeklischee, Versandinformationen (Wahl-  
10 drucke) und zusätzlichen editierbaren Mitteilungen. Der nichtflüchtige Speicher NVM 94 weist eine Vielzahl an Speicherbereichen auf. Darunter sind solche, welche die geladenen Portogebührentabellen nichtflüchtig speichern.

15 Die Chipkarten-Schreib/Leseinheit 70 besteht aus einem zugehörigen mechanischen Träger für die Mikroprozessorkarte und Kontaktiereinheit 74. Letztere gestattet eine sichere mechanische Halterung der Chipkarte in Lese-Position und eindeutige Signalisierung des Erreichens der Lese-Position der Chipkarte in der Kontaktierungseinheit. Die Mikro-  
20 zessorkarte mit dem Mikroprozessor 75 besitzt eine einprogrammierte Lesefähigkeit für alle Arten von Speicherkarten bzw. Chipkarten. Das Interface zur Frankiermaschine ist eine serielle Schnittstelle gemäß RS232-Standard. Die Datenübertragungsrate beträgt min. 1,2 K Baud. Das Einschalten der Stromversorgung erfolgt mittels einem an der Haupt-  
25 platine angeschlossenen Schalter 71. Nach Einschalten der Stromversorgung erfolgt eine Selbsttestfunktion mit Bereitschaftsmeldung.

In der Figur 3 ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter 1 und  
30 einer Base 2. Letztere ist mit einer Chipkarten-Schreib/ Leseinheit 70 ausgestattet, die hinter der Führungsplatte 20 angeordnet und von der Gehäuseoberkante 22 zugänglich ist. Nach dem Einschalten der Frankiermaschine mittels dem Schalter 71 wird eine Chipkarte 49 von oben nach unten in den Einsteckschlitz 72 eingesteckt. Ein zugeführter auf der Kante  
35 stehender Brief 3, der mit seiner zu bedruckenden Oberfläche an der Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit einem Sicherheitabdruck 31 bedruckt. Die Briefzuführöffnung wird durch eine Klarsichtplatte 21 und die Führungsplatte 20 seitlich begrenzt. Die

Statusanzeige des auf die Hauptplatine 9 des Meters 1 gesteckten Sicherheitsmoduls 100 ist von außen durch eine Öffnung 109 sichtbar.

Die Figur 4 zeigt eine Darstellung eines Sicherheitsabdrucks, wie er von  
5 der amerikanischen USPS gefordert wird. Der Sicherheitsabdruck ist  
rechts vom Werbeklischee angeordnet und weist in der oberen Hälfte ein  
Beförderer-Logo und den Portowert und in der unteren Hälfte das Datum,  
den Portowert, einen Key-Indicator und einen Datenauthentisierungscode  
DAC in einer ersten Zeile und eine Hersteller-ID, eine Maschinen-ID, eine  
10 Modell-ID und den Ascendungsregisterwert in einer zweiten Zeile auf,  
wobei beide Zeilen maschinenlesbar sind. Beide maschinenlesbare Zeilen  
sind durch Markierungsbalken seitlich begrenzt, welche die Erkennung  
und Auswertung der Zeichen nach dem OCR-Verfahren verbessern. Ein  
entsprechendes Auswerteverfahren für die vorgenannten Daten, die die  
15 Zeichen wiedergeben, wurde bereits in der europäischen Anmeldung EP  
862 143 A2 zur Überprüfung eines Sicherheitsabdruckes vorgeschlagen.

Erfindungsgemäß wird die Berechnung des DAC für den Sicherheits-  
abdruck im Sicherheitsmodul durchgeführt. Eine weitere Beschleunigung  
20 der Berechnung des Sicherheitscodes wird durch die Wahl eines eigens  
für die DES-Berechnung gewählten und zertifizierten Assembler-  
Algorithmus erzielt.

Um auch Druckdaten, die lediglich Teile eines Datums angeben, durch  
25 eine OCR-Lesestation authentifizieren zu können, wird für diese  
speziellen Datums-Werte ein *Left out-Wert* definiert. Dieser wird anstelle  
des Datumeintrages verwendet. Beispielsweise wird der Wert 0  
verwendet, wenn die entsprechende Datumsteile nicht vorliegen.

Um das Druckdatum auf Gültigkeit zu prüfen, ist die Speicherung des  
30 aktuellen Datums in zwei unterschiedlichen Formaten und  
Speicherplätzen notwendig, da das Format der SM-internen Echtzeituhr  
RTC sich vom Format des im Druckbild verwendeten Datums  
unterscheidet und ein Vergleich zum Zeitpunkt der Abrechnung  
35 entsprechend Zeit benötigt.

Der Aufbau und die Interpretation der Systemdaten, die in den  
Sicherheitscode eingehen, sowie die Systemdaten, die von der FM für  
den Druck genutzt werden ermöglicht eine weitere Beschleunigung.

Da bei Massenfrankierungen das Druckdatum in der Regel konstant bleibt, lassen sich die ersten 8 Bytes des Sicherheitscodes in einer ersten 3DES-Runde für jeden Tag vorabrechnen.

- 5 In der Tafel 1 wird ein weiteres Beispiel für die Daten aus einem Sicherheitsabdruck hervorgehen gezeigt.

**Tafel 1 :**

#	Information	Value range		Left out	Leading zeroes
1.		Lower	Upper		
2.	Date of mailing Month:	JAN	DEC	'...'	
3.	Day:	01	31	'..'	YES
4.	Year:	1999		'....'	
5.	Postage	00000	99999		YES
6.	Key-Indicator	0	9		
7.	Data Authentication Code	00000	65535		YES
8.	Vendor ID	FP			
9.	Machine ID	0000001	9999999		YES
10.	Model ID	JMB01	JMB99		
11.	Ascending Register	00000000	FFFFFFFF		YES

- 10 Die Tafel 2 verdeutlicht Systemdaten die in den Sicherheitscode eingehen und gibt die Länge der benötigten Bytes an und Tafel 3 zeigt ein Beispiel..

**Tafel 2:**

	Element	Byte-Länge	Wertebereich (dezimal)
1.	Maschinen- ID	4	7 digit -Wertebereich für Francotyp-Postalia
2.	OCR Key Indicator	1	0..9
3.	Postdatum Subelemente: Jahr Monat Tag	Total: 3 Detail: 1 1 1	0..99 , 0..12 , 0..31 ,
4.	Portowert	4	0..99999 (unit is 1/10 cents)
5.	Ascending Register	4	0..4294967295 (unit is 1/10 cents)
	<b>TOTAL:</b>	<b>16</b>	

**Tafel 3: Beispiel für den Aufbau eines Sicherheitscodes**

	Serien-Nummer					KI	Postdatum			Portowert				Ascending Register			
Dezimale Daten	0050010					1	Feb 17 1999			\$12.300				\$129.300			
Hex. Daten	00	00	C3	5A	01	63	02	11	00	00	30	0C	00	1F	91	14	

Die Figur 5 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls PSM 100 in einer bevorzugten Variante. Der negative Pol der Batterie 134 ist auf Masse und einen Pin P23 der Kontaktgruppe 102 gelegt. Der positive Pol der Batterie 134 ist über die Leitung 193 mit dem einen Eingang des Spannungsumschalters 180 und die Systemspannung führende Leitung 191 ist mit dem anderen Eingang des Spannungsumschalters 180 verbunden. Als Batterie 134 eignet sich der Typ SL-389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM 100. Als Spannungsumschalter 180 kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 an der Batterieüberwachungseinheit 12 und der Detektionseinheit 13 an. Die Batterieüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins 1, 2, 4 und 5 des Prozessors 120 über die Leitungen 135, 164 und 137, 139 in Kommunikationsverbindung. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 außerdem am Versorgungseingang eines ersten Speichers SRAM 116 an, der durch die vorhandene Batterie 134 zum nichtflüchtigen Speicher NVRAM einer ersten Technologie wird.

Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus 115, 117, 118 in Verbindung. Der Prozessor 120 kann über den Systembus und ein Modem 83 in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC 150 vollzogen. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher Technologie gespeichert.

Am Versorgungseingang eines zweiten Speichers NV-RAM 114 liegt Systemspannung an. Hierbei handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOW-RAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM 114 der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC's 150 über einen internen Adreß- und Datenbus 112, 113 verbunden.

Der ASIC 150 enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) 160 ist eine Zugriffslogik auf den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine 9 ist an



entsprechenden Pins der Logik PAL 160 angeschlossen und die PAL 160 erzeugt mindestens ein Steuersignal für das ASIC 150 und ein Steuersignal 119 für den Programmspeicher FLASH 128. Der Prozessor 120 arbeitet ein Programm ab, das im FLASH 128 gespeichert ist. Der  
5 Prozessor 120, FLASH 28, ASIC 150 und PAL 160 sind über einen modulinternen Systembus miteinander verbunden, der Leitungen 110, 111, 126, 119 für Daten-, Adreß- und Steuersignale enthält.

Die RESET-Einheit 130 ist über die Leitung 131 mit dem Pin 3 des Prozessors 120 und mit einem Pin des ASIC's 150 verbunden. Der  
10 Prozessor 120 und das ASIC 150 werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit 130 zurückgesetzt.

15 An den Pins 6 und 7 des Prozessors 120 sind Leitungen angeschlossen, welche nur bei einem an die Hauptplatine 9 gesteckten PSM 100 eine Leiterschleife 18 bilden.

Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine  
20 Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf. An den Pins 8 und 9 liegen I/O-Ports der Ein/Ausgabe-Einheit 125, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED's 107, 108, welche den Zustand des Sicherheitsmoduls 100 signalisieren. Die Sicherheitsmodule  
25 können in ihrem Lebenszyklus verschiedene Zustände einnehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der  
30 Implementierung abhängig.

Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen modulinternen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 dient als Programmspeicher und wird mit  
35 Systemspannung  $U_{s+}$  versorgt. Er ist beispielsweise ein 128 Kbyte-FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC 150 des postalischen Sicherheitsmoduls 100 liefert über einen modulinternen Adreßbus 110 die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH 128. Der Prozessor 120 des Sicherheitsmoduls 100

5 liefert über einen internen Adreßbus 111 die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH 128. Der ASIC 150 des Sicherheitsmoduls 100 steht über die Kontaktgruppe 101 des Interfaces 8 mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 der Hauptplatine 9 in Kommunikationsverbindung.

10 Die Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Diese Spannung wird von der Spannungsüberwachungseinheit (Battery Observer) 12 erzeugt. Letzterer liefert außerdem ein Statussignal 164 und reagiert auf ein Steuersignal 135. Der Spannungsumschalter 180 gibt als Ausgangs-  
15 spannung auf der Leitung 136 für die Spannungsüberwachungseinheit 12 und Speicher 116 diejenige seiner Eingangsspannungen weiter, die größer als die andere ist. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen  $U_{s+}$  und  $U_{b+}$  automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie 134 ohne Datenverlust gewechselt werden.

20 Die Batterie der Frankiermaschine speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr 122 mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) 124, der sicherheitsrelevante Daten hält. Sinkt die Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der im Ausführungsbeispiel beschriebenen Schaltung der Speisepunkt für  
25 RTC und SRAM mit Masse verbunden. D.h. die Spannung an der RTC und am SRAM liegt dann bei 0V. Das führt dazu, daß der SRAM 124, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig werden auch die Register der RTC 122 gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch diese  
30 Aktion wird verhindert, daß ein möglicher Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr 122 anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß er Sicherheitsmaßnahmen, wie beispielsweise Long Time Watchdogs umgeht.

35 Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die beschriebene Schaltung in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung abfragen (Statussignal) und damit und/oder über die Auswertung der

Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung zurücksetzen, d.h. "scharf" machen.

5

Weitere Maßnahmen zum Schutz eines Sicherheitsmoduls vor einem Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht vorveröffentlichten deutschen Anmeldungen 198 16 572.2 8 mit dem Titel: Anordnung für ein Sicherheitsmodul und 198 16 571.4 mit dem Titel: Anordnung für den Zugriffsschutz für Sicherheitsmodule, sowie 199 12 780. 8 mit dem Titel: Anordnung für ein Sicherheitsmodul, 199 12 781.6 mit dem Titel: Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens und die deutsche Gebrauchsmusteranmeldung 299 05 219.2 mit dem Titel: Sicherheitsmodul mit Statussignalisierung vorgeschlagen. Ein steckbares Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen. Es kann nun unterschieden werden, ob das Sicherheitsmodul funktioniert oder defekt ist. Dabei wird auf die Nichtmanipulierbarkeit der hardwaremäßigen Abrechnung vertraut, ohne dies noch einmal zu kontrollieren. Jede andere softwaregesteuerte Arbeitsweise gilt nur mit den Originalprogrammen als fehlerfrei, welche deshalb vor einer Manipulation geschützt werden müssen.

Die erste Datenverarbeitungseinheit 120 ist erfindungsgemäß durch ein im Programmspeicher 128 des Sicherheitsmoduls gespeichertes Programm programmiert, den Datenauthorisierungscode DAC vorauszuberechnen und an die separate Datenverarbeitungseinheit  $\mu P$ , 91 zu übermitteln, die parallel und annähernd zeitgleich zur Operation der Vorausberechnung durch ein Programm in ihrem Programmspeicher 92 zu einer Druckdatenaufbereitung und zur Berechnung eines Druckbildes programmiert ist. Es ist vorgesehen, daß die erste Datenverarbeitungseinheit 120 des Sicherheitsmoduls 100 einen internen nichtflüchtigen Speicher 124 aufweist, in welchem mindestens ein Schlüssel für die Berechnung des Datenauthorisierungscode (DAC) vor einem Zugriff geschützt gespeichert ist. Im Sicherheitsmodul 100 ist eine zweite Datenverarbeitungseinheit 150 für eine Abrechnung der Postregister vorgesehen, so daß die vom Sicherheitsmodul 100 separate Datenverarbeitungseinheit im Meter eine dritte Datenverarbeitungseinheit  $\mu P$ , 91 insbesondere für die Bearbeitung der Druckaufgaben bildet.

In der zweiten Datenverarbeitungseinheit ASIC 150 ist eine Hardware-abrechnungseinheit zur Durchführung der Abrechnung enthalten, welche den neuen Postregistersatz mit den Abrechnungsdaten in den nichtflüchtigen Speicher 114, 116 einspeichert.

5

Die erste Datenverarbeitungseinheit ist ein Modulprozessor 120 des Sicherheitsmoduls, welcher vorzugsweise programmiert ist, die ersten 8 Bytes des Datenauthorisierungscode (DAC) nach einem Algorithmus in einer ersten Runde für jeden Tag vorauszuberechnen. Der Algorithmus für  
10 den Datenauthorisierungscode (DAC) schließt einen DES-Algorithmus, insbesondere einen Tripel-DES-Algorithmus (3DES) ein.

Der Modulprozessor 120 des Sicherheitsmoduls ist programmiert, bei Einzelpostverarbeitung nach Eingabe eines Portowertes den Daten-  
15 authorisierungscode (DAC) vorauszuberechnen bzw. bei Massenpostverarbeitung nach Abrechnung des vorhergehenden Portowertes den nächstfolgenden Datenauthorisierungscode (DAC) vorauszuberechnen, wenn der Portowert nicht geändert wird und nach Vorausberechnung den Datenauthorisierungscode (DAC) an die dritte Datenverarbeitungseinheit  
20 µP, 91 sofort zu übermitteln.

Der interne nichtflüchtige Speicher 124 ist ein durch eine Batterie 134 gestützter SRAM-Speicher des Modulprozessors 120 und ist mit Bereichen zur geschützten Speicherung von mindestens einen Teil der  
25 Daten eines Postregistersatzes ausgebildet, welcher bei einer Vorausberechnung entsteht. In einem der Speicherbereiche ist der für die Berechnung eines Datenauthorisierungscode (DAC) erforderliche mindestens eine Schlüssel geschützt gespeichert.

30 Der Modulprozessor 120 des Sicherheitsmoduls 100 ist programmiert, mit dem Portowert den steigenden Registerwert R2 (ascending register) im Voraus zu bestimmen und unter Einbeziehung des ermittelten Wertes den Datenauthorisierungscode (DAC) für die Daten des Sicherheitsabdruckes vorauszuberechnen. Beispielsweise unter Einbeziehung folgender Daten  
35 des Sicherheitsabdruckes kann der Datenauthorisierungscode (DAC) vorausberechnet werden: Maschinen-Identifikation, OCR-Key-Indikator, Datum, Postwert und Registerwertes R2 für das steigende Register, der bei der Vorausberechnung ermittelt wurde.

Das Verfahren zur Generierung eines Sicherheitsabdruckes besteht im Wesentlichen in den Schritten:

- Vorausberechnung des aufsteigenden Registerwertes R2,
- Vorausberechnung des Datenauthorisierungscode,
- 5 - Übermittlung des Datenauthorisierungscode an eine separate Datenverarbeitungseinheit  $\mu P$ , 91, welche ausgebildet ist, die Druckdaten extern des Sicherheitsmoduls 100 aufzubereiten, daß Druckbild zu berechnen und auszudrucken.

10 Anhand des - in der Figur 6 dargestellten - Flußdiagramms werden nun die Routinen näher erläutert, welche im System vor dem Frankieren ablaufen. Der Mikroprozessor CPU 121 ist durch ein entsprechendes im Flash 128 gespeichertes Programm programmiert, solche vorgenannten Selbsttests auszuführen, wobei nach dem Start 299, in einem ersten  
15 Schritt 300 ein Power on-Selbsttest durchgeführt und dann im Schritt 301 gefragt wird, ob der Power on-Selbsttest ein OK ergeben hat. Ist das der Fall, so wird im Schritt 302 die grüne LED 107 vom Mikroprozessor CPU 121 über ein I/O-Port 125 leuchtend gesteuert. Anderenfalls wird im Schritt 303 die rote LED 108 vom Mikroprozessor CPU 121 über ein I/O-  
20 Port 125 leuchtend gesteuert.

Vom Schritt 302 wird auf die Abfrage 304 verzweigt, in welcher geprüft wird, ob eine weitere statische Prüfung verlangt wird. Ist das der Fall, so wird zum Schritt 300 zurückverzweigt. Anderenfalls wird auf die Abfrage 305 verzweigt, in welcher geprüft wird, ob durch einen Briefsensor eine  
25 Briefanlage festgestellt bzw. vom Modulprozessor 120 eine Eingabe einen neuen Portowertes erkannt wird. Ist dies beides nicht der Fall, dann wird auf den Schritt 302 zurückverzweigt und somit eine Warteschleife solange durchlaufen, bis eine Briefanlage/Neueingabe festgestellt worden ist. Im letzteren Fall wird auf den Schritt 306 verzweigt, um das Eingeben der  
30 Daten zu beenden. Gleichzeitig oder kurz nach dem Zeitpunkt  $t_0$  beginnend, wird ein Schritt 307 zur MAC-Berechnung auf der Grundlage der zum Zeitpunkt  $t_0$  verfügbaren Postregisterdaten  $P'_{t_0}$  gestartet. Ein vom Modulprozessor 120 bereits früher gebildeter  $MAC(P_{t_0})$  ist zum Zeitpunkt  $t_0$  gültig. Die MAC-Berechnung ist zum Zeitpunkt  $t_1$  abgeschlossen. Der  
35 berechnete  $MAC(P'_{t_0})$  wird mit dem alten zum Zeitpunkt  $t_0$  gültigen (vom Modulprozessor 120 bereits früher gebildeten)  $MAC(P_{t_0})$  zum Zeitpunkt  $t_1$  im Schritt 308 verglichen. Bei Nichtübereinstimmung wird zum Schritt 315 verzweigt, um die LED's 107, 108 orange leuchtend zu steuern. Anderenfalls wird zum Schritt 309 verzweigt. Dort erfolgt zum Zeitpunkt  $t_2$

im Modulprozessor 120 eine Vorausberechnung des aufsteigenden Registerwertes  $R_{t_2}$  und eine  $DAC_{neu}$ -Berechnung. Anschließend erfolgt im Schritt 310 eine Vorausberechnung des Postregistersatzes  $P_{t_2}$  eine  $MAC_{neu}$ -Bildung, ggf. mit Speicherung im NVRAM\_P 124. Die Voraus-

5 berechnung des Datenauthorisierungscode (DAC) bezieht den aufsteigenden Registerwert R2 und weitere Daten ab einem Zeitpunkt  $t_{i+1}$  ein, der nach dem Dateneingabe-Ende und/oder bei Massenfrankierungen ab Anlage eines weiteren Poststücks und vor der eigentlichen Abrechnung (312) liegt. Von den weiteren Daten, die mindestens den Portowert p und

10 das Datum einschließen, kann mindestens die Maschinen-ID und ggf. das Datum in die DAC-Vorausberechnung ab Anlage eines weiteren Poststücks (Zeitpunkt  $t_0$ ) einbezogen werden, wenn es für den jeweiligen zu frankierenden Briefstapel unverändert bleibt. Bis zum Zeitpunkt  $t_5$  ist die Generierung im Sicherheitsmodul abgeschlossen.

15 Zum Zeitpunkt  $t_3$ , wenn im Schritt 311 die Speicherung des  $MAC(P_{t_2})$  im NVRAM\_P von der einen Datenverarbeitungseinheit 120 abgeschlossen worden ist, wird von der anderen Datenverarbeitungseinheit, nämlich von der – in der Figur 5 gezeigten – Hardware-Abrecheneinheit im ASIC 150 im Schritt 312 eine Berechnung des neuen Postregistersatzes

20 durchgeführt.

In einem abschließenden Schritt 313 erfolgt eine Abspeicherung der Ergebnisse  $P'_{t_3}$  und  $MAC(P_{t_2})$  im NVRAM\_A. In Vorbereitung eines Frankierens können dann noch eine Anzahl von weiteren Schritten seriell oder parallel zu den vorgenannten Schritten durchlaufen werden, die

25 mindestens einen Subschritt zum Generieren eines Sicherheitscodes DAC einschließen und die mit einem Schritt 314 zur Druckdatenbereitstellung zum Frankieren des Briefes abschließen. Letzterer beinhaltet mindestens jedoch das Senden des Sicherheitscodes DAC an den Mikroprozessor 91 des Meters. Anschließend wird zum Schritt 302 zurückverzweigt.

30 Zum Generieren eines DAC-Sicherheitscodes wird zwar ebenfalls eine prinzipiell gleiche MAC-Bildungsprozedure genutzt, der DAC setzt sich aber aus dem Ascending-Registerwert R2 und aus weiteren Daten zusammen (Maschinen-ID, OCR-Key-Indikator, Datum, Portowert p) und das Generieren erfolgt zu einem anderem Zeitpunkt  $t_{i+1}$  zum Beispiel ab

35 Dateneingabe-Ende. Bei Massenfrankierungen ist im Anschluß der Übermittlung des Datenauthorisierungscode an die separate Datenverarbeitungseinheit  $\mu P$  91 vorgesehen, daß vom Modulprozessor 120 der nächstfolgende Datenauthorisierungscode (DAC) vorausberechnet wird.

Der Modulprozessor 120 arbeitet mit dem – in der Figur 5 gezeigten – Steuerungsprozessor  $\mu P$  91 des Meters zusammen, wobei letzterer mindestens den Sicherheitscode  $DAC(R2_{t(i+1)})$ , weitere Daten) empfängt, die Druckdaten zusammenstellt und zum Druckkopf übermittelt.

5

Erfindungsgemäß ist das Sicherheitsmodul zum Einsatz in postalischen Geräten bestimmt, insbesondere zum Einsatz in einer Frankiermaschine. Jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es mit einem Personalcomputer zusammenarbeiten kann, der als dritte Dateiverarbeitungseinheit fungiert. Es kann beispielsweise mit die Hauptplatine eines Personalcomputers verbunden werden, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

10

15

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Schutzansprüchen umfaßt werden.

\*\*\*

20

### Zusammenfassung

Die Erfindung betrifft eine Anordnung und Verfahren zur Generierung eines Sicherheitsabdruckes. Das Verfahren schließt die Schritte

5 Vorausberechnung (306-311, 316-322) des aufsteigenden Registerwertes R2 und eines Datenauthorisierungscode (DAC) sowie seine Übermittlung (314, 324) an eine separate Datenverarbeitungseinheit ( $\mu$ P) ein. Die Anordnung hat einen Sicherheitsmodul (SM), der einen Programmspeicher (128), mindestens eine erste Datenverarbeitungseinheit (120)

10 und nichtflüchtige Speicher (114, 116) einschließt, wobei die erste Datenverarbeitungseinheit (120) mit dem nichtflüchtigen Speicher (114, 116) für die Postregisterdaten verbindbar ist. Die erste Datenverarbeitungseinheit (120) ist durch ein Programm im Programmspeicher (128) programmiert, den Datenauthorisierungscode (DAC) vorauszuberechnen und an die

15 separate Datenverarbeitungseinheit ( $\mu$ P) zu übermitteln, welche durch ein Programm in ihrem Programmspeicher (92) zu einer Druckdatenaufbereitung und zur Berechnung eines Druckbildes programmiert ist.

Fig. 1b

\*\*\*



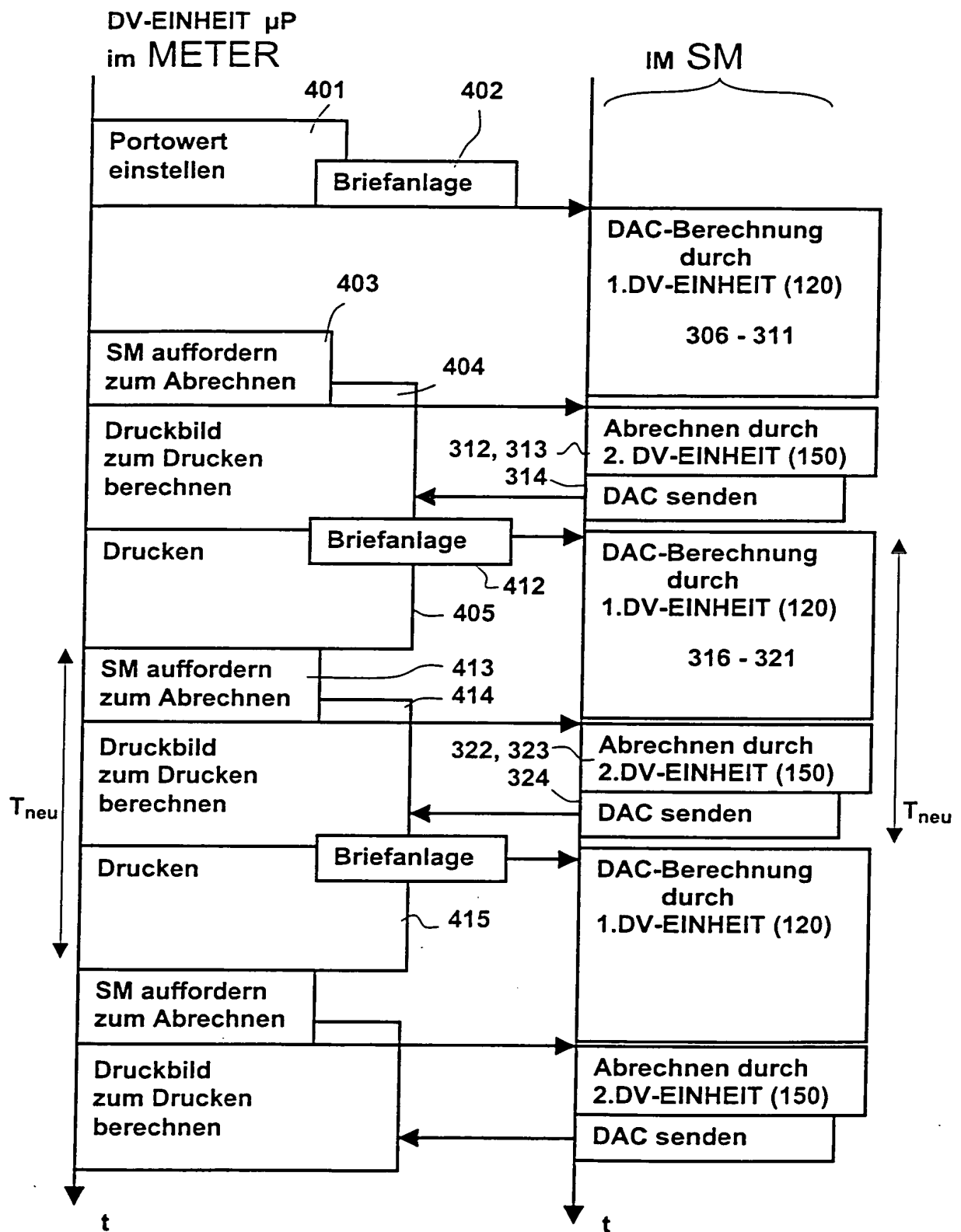


Fig. 1b

Patentansprüche

1. Anordnung zur Generierung eines Sicherheitsabdruckes, mit einem  
5 Sicherheitsmodul, der einen Programmspeicher (128), mindestens eine  
erste Datenverarbeitungseinheit (120) und nichtflüchtige Speicher (114,  
116) einschließt, wobei die erste Datenverarbeitungseinheit (120) mit dem  
nichtflüchtigen Speicher (114, 116) für die Postregisterdaten verbindbar  
ist, g e k e n n z e i c h n e t d a d u r c h, daß die erste Daten-  
10 verarbeitungseinheit (120) durch ein Programm im Programmspeicher  
(128) programmiert ist, einen Datenauthorisierungscode (DAC) für Daten  
des Sicherheitsabdruckes vorauszuberechnen bevor eine Abrechnung  
erfolgt und an eine separate Datenverarbeitungseinheit ( $\mu$ P, 91) zu über-  
mitteln, wobei die separate Datenverarbeitungseinheit ( $\mu$ P, 91) durch ein  
15 Programm in ihrem Programmspeicher (92) zu einer Druckdaten-  
aufbereitung und zur Berechnung eines Druckbildes programmiert ist.

2. Anordnung, nach Anspruch 1, g e k e n n z e i c h n e t d a d u r c h,  
20 daß die erste Datenverarbeitungseinheit (120) des Sicherheitsmoduls  
einen internen nichtflüchtigen Speicher (124) aufweist, in welchem  
mindestens ein Schlüssel für die Berechnung des Datenauthorisierungs-  
codes (DAC) vor einem Zugriff geschützt gespeichert ist und daß der  
Sicherheitsmodul eine zweite Datenverarbeitungseinheit (150) für eine  
25 Abrechnung der Postregister aufweist sowie daß die separate Daten-  
verarbeitungseinheit eine dritte Datenverarbeitungseinheit ( $\mu$ P, 91) bildet.

3. Anordnung, nach den Ansprüchen 1 bis 2, g e k e n n z e i c h n e t  
30 d a d u r c h, daß die erste Datenverarbeitungseinheit ein Modulprozessor  
(120) des Sicherheitsmoduls (100) ist, welcher programmiert ist, die  
ersten acht Bytes des Datenauthorisierungscode (DAC) nach einem  
Algorithmus in einer ersten Runde für jeden Tag vorauszuberechnen.

4. Anordnung, nach den Ansprüchen 1 bis 3, gekennzeichnet dadurch, daß der Algorithmus für den Datenauthorisierungscode (DAC) einen DES-Algorithmus einschließt.

5

5. Anordnung, nach den Ansprüchen 1 bis 4, gekennzeichnet dadurch, daß der Algorithmus für den Datenauthorisierungscode (DAC) einen Tripel-DES-Algorithmus (3DES) einschließt.

10

6. Anordnung, nach Anspruch 1, gekennzeichnet dadurch, daß der Modulprozessor (120) des Sicherheitsmoduls programmiert ist, bei Einzelpostverarbeitung nach Eingabe eines Portowertes den Datenauthorisierungscode (DAC) vorauszuberechnen.

15

7. Anordnung, nach Anspruch 1, gekennzeichnet dadurch, daß der Modulprozessor (120) des Sicherheitsmoduls programmiert ist, bei Massenpostverarbeitung nach Abrechnung des vorhergehenden Portowertes den nächstfolgenden Datenauthorisierungscode (DAC) vorauszuberechnen, wenn der Portowert nicht geändert wird und nach Vorausberechnung den Datenauthorisierungscode (DAC) an die dritte Datenverarbeitungseinheit ( $\mu P$ , 91) sofort zu übermitteln.

25

8. Anordnung, nach Anspruch 2, gekennzeichnet dadurch, daß der interne nichtflüchtige Speicher (124) ein durch eine Batterie (134) gestützter SRAM-Speicher des Modulprozessors (120) ist und mit Bereichen zur geschützten Speicherung von mindestens einen Teil der Daten eines Postregistersatzes ausgebildet ist, der bei einer Vorausabrechnung entsteht, daß in einem der Speicherbereiche der mindestens eine Schlüssel für die Berechnung des Datenauthorisierungscode (DAC) geschützt gespeichert ist.

30

9. Anordnung, nach einem der vorhergehenden Ansprüche 1 bis 8, gekennzeichnet dadurch, daß der Modulprozessor (120) programmiert ist, mit dem Portwert den steigenden Registerwert im Voraus zu bestimmen und unter Einbeziehung des ermittelten Wertes den  
5 Datenauthorisierungscode (DAC) vorauszuberechnen.

10. Anordnung, nach Anspruch 9, gekennzeichnet dadurch, daß der Modulprozessor (120) des Sicherheitsmoduls programmiert ist, unter Einbeziehung einer Maschinen-Identifikation, eines OCR-Schlüssel-  
10 Indikators, eines Datums, des Postwertes und des bei der Vorausabrechnung ermittelten Registerwertes für das steigende Register den Datenauthorisierungscode (DAC) vorauszuberechnen.

15 11. Anordnung, nach Anspruch 2, gekennzeichnet dadurch, daß eine Hardwareabrechnungseinheit in der zweiten Datenverarbeitungseinheit (150) zur Durchführung der Abrechnung enthalten ist, welche den neuen Postregistersatz mit den Abrechnungsdaten in den  
20 nichtflüchtigen Speicher (114, 116) einspeichert.

25 12. Verfahren zur Generierung eines Sicherheitsabdruckes, mit einer Authorisierungscode-Berechnung zur Sicherung der Postregister vor Manipulation durch eine erste Datenverarbeitungseinheit und mit einer Abrechnung durch eine zweite Datenverarbeitungseinheit im Sicherheitsmodul, gekennzeichnet durch die Schritte:

- Vorausberechnung des aufsteigenden Registerwertes R2,
- Vorausberechnung des Datenauthorisierungscode (DAC),
- 30 - Übermittlung des Datenauthorisierungscode an eine separate Datenverarbeitungseinheit ( $\mu P$ , 91), welche ausgebildet ist, die Druckdaten extern des Sicherheitsmoduls (100) aufzubereiten, daß Druckbild zu berechnen und auszudrucken.

13. Verfahren, nach Anspruch 12, gekennzeichnet dadurch,  
daß die Vorausberechnung des Datenauthorisierungs-  
codes (DAC), den aufsteigenden Registerwert R2 und weitere Daten einbezieht und daß das  
Generieren zu einem Zeitpunkt  $t_{i+1}$  ab Dateneingabe-Ende und/oder bei  
5 Massenfrankierungen ab Anlage eines weiteren Poststücks und vor der  
eigentlichen Abrechnung erfolgt.

14. Verfahren, nach Anspruch 13, gekennzeichnet dadurch,  
10 daß die weiteren Daten mindestens die Maschinen-ID, den Portowert p  
und das Datum einschließen, wobei mindestens die Maschinen-ID und  
optional das Datum in die Vorausberechnung einbezogen wird, wenn es  
es für den jeweiligen zu frankierenden Briefstapel unverändert bleibt.

15  
15. Verfahren, nach den Ansprüchen 12 bis 24, gekennzeichnet  
dadurch, daß bei Massenfrankierungen im Anschluß der Übermittlung  
des Datenauthorisierungs-  
codes an die separate Datenverarbeitungse-  
inheit ( $\mu P$ , 91), vom Modulprozessor (120) der nächstfolgende  
20 Datenauthorisierungscode (DAC) vorauszuberechnet wird.

\*\*\*\*\*

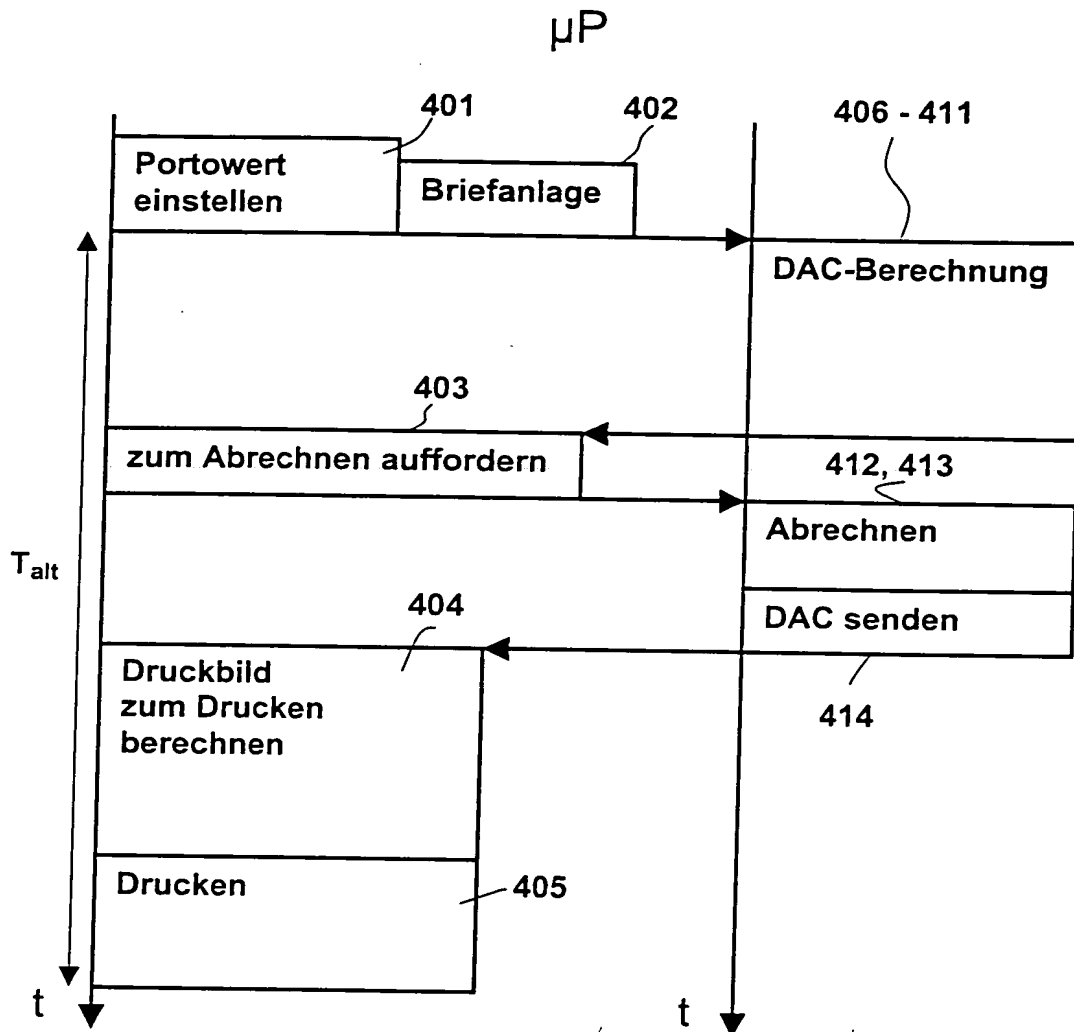


Fig. 1a

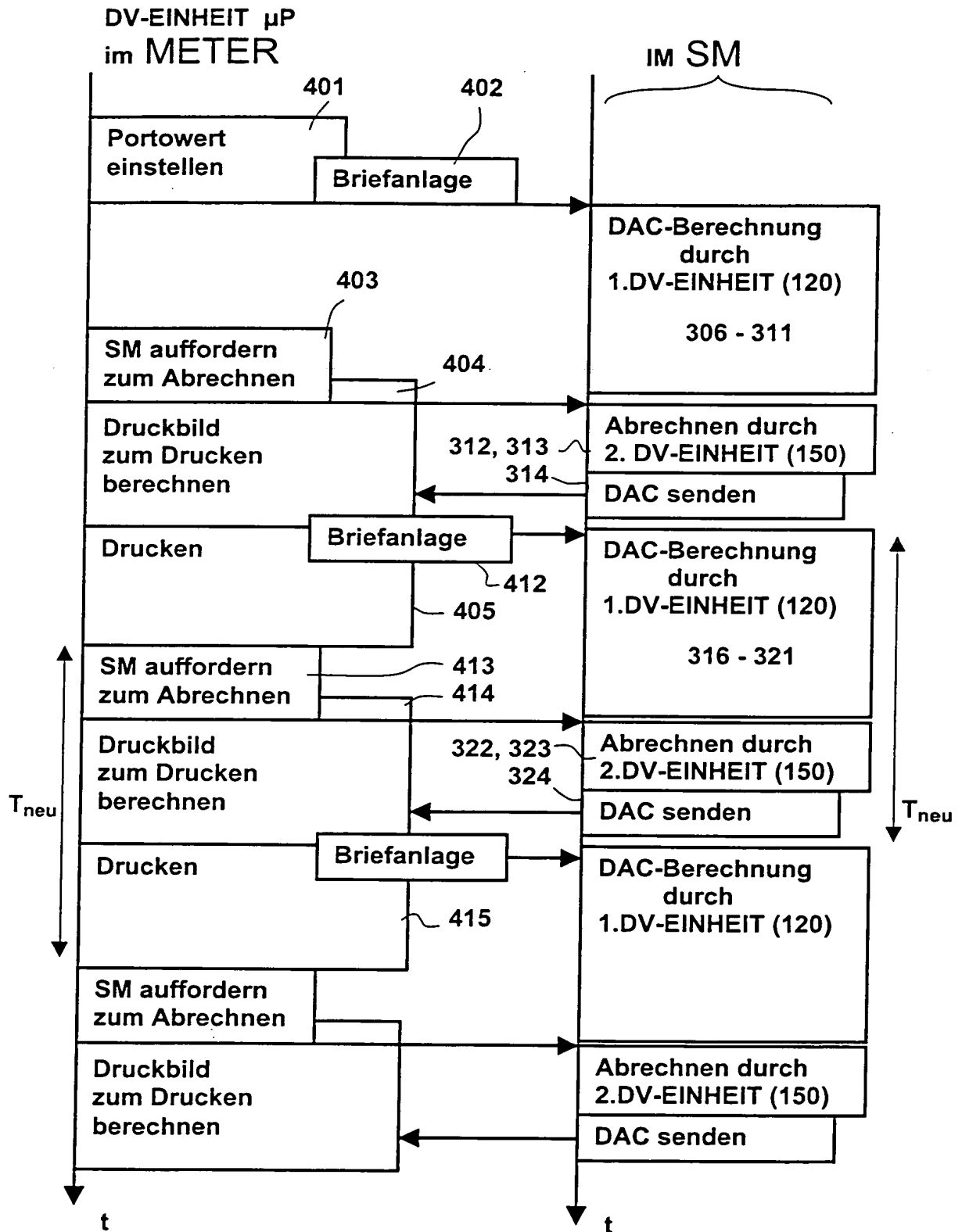


Fig. 1b

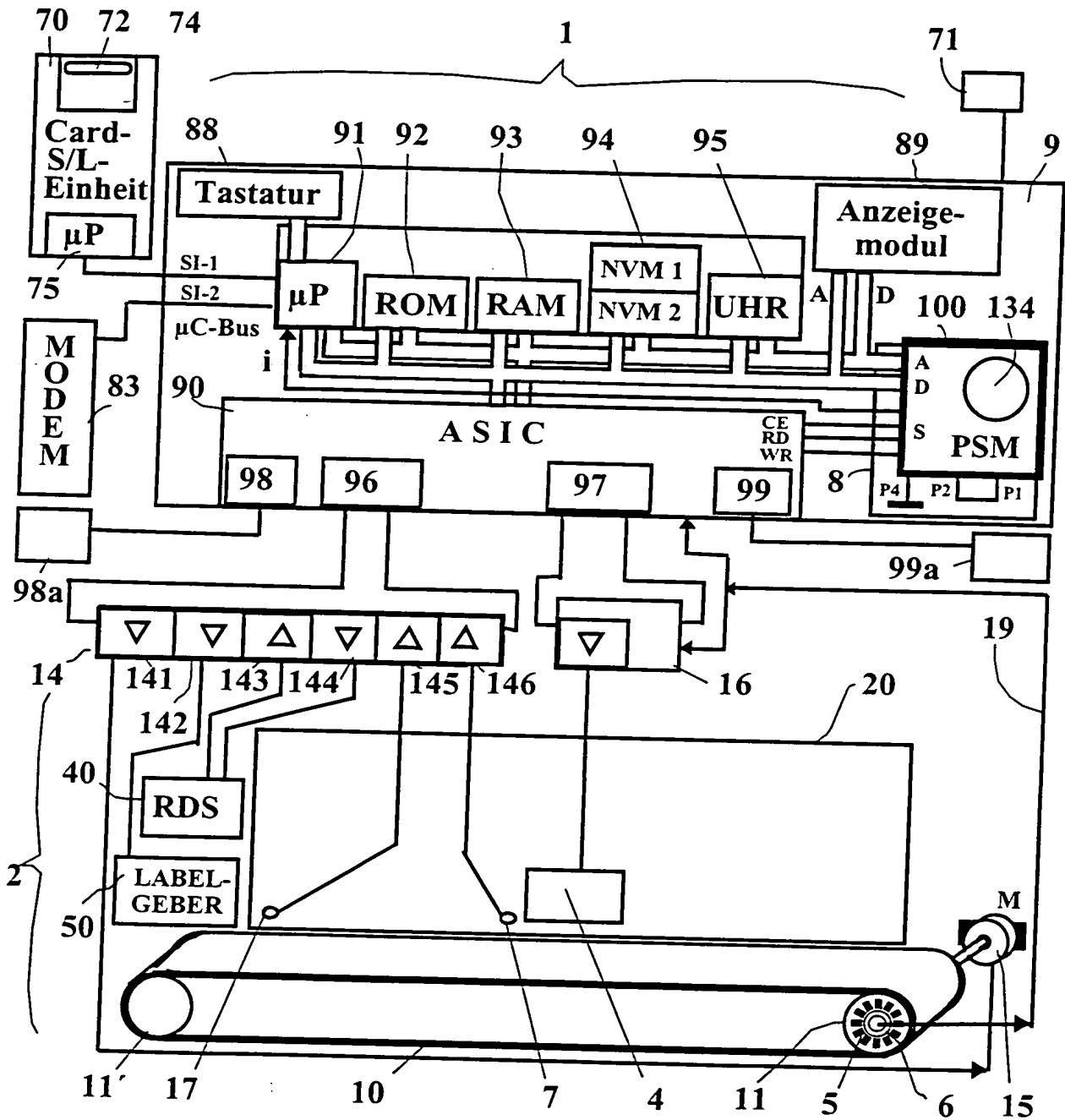


Fig. 2



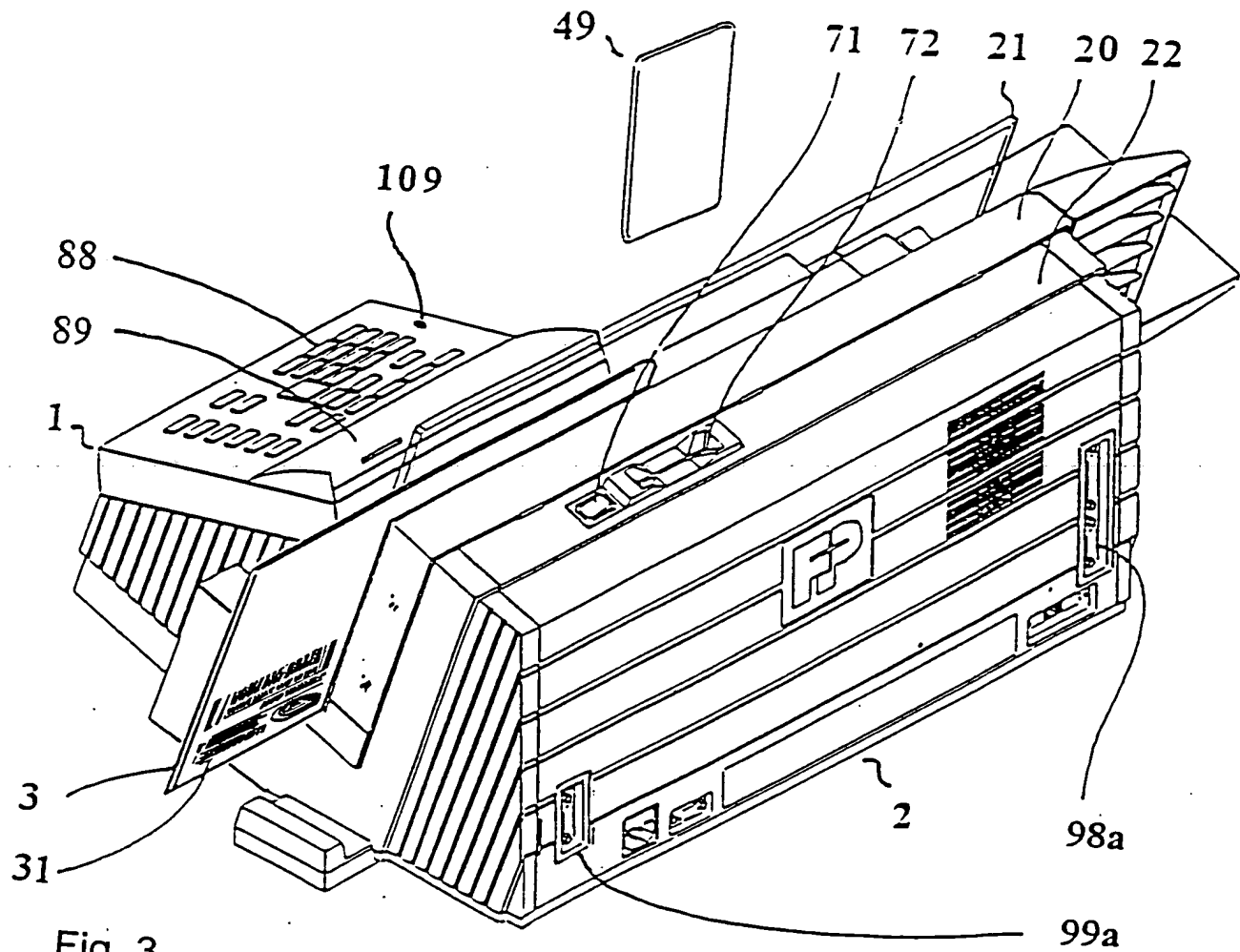


Fig. 3

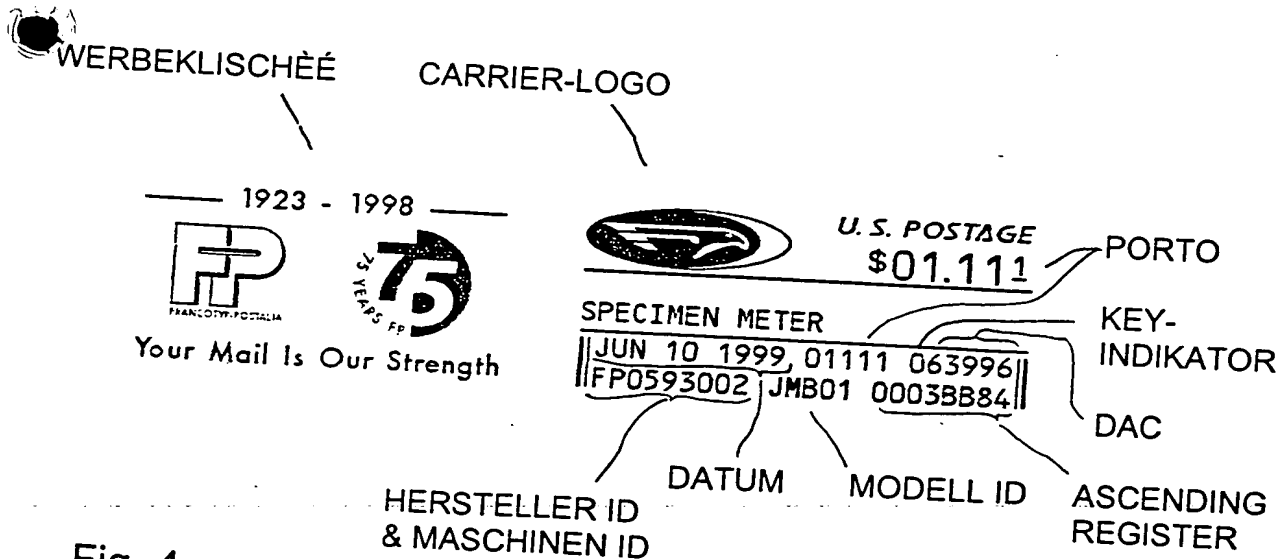


Fig. 4

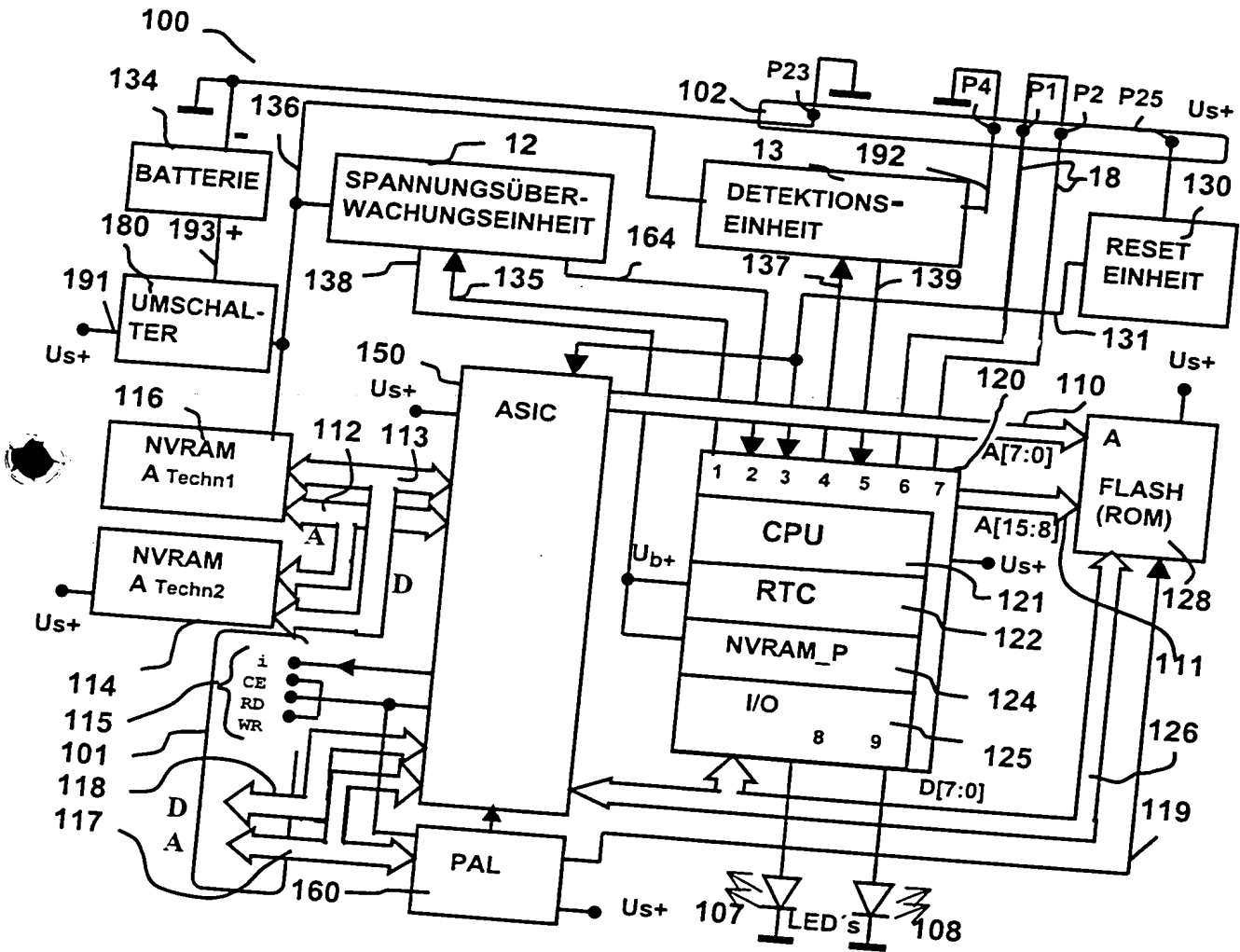


Fig. 5

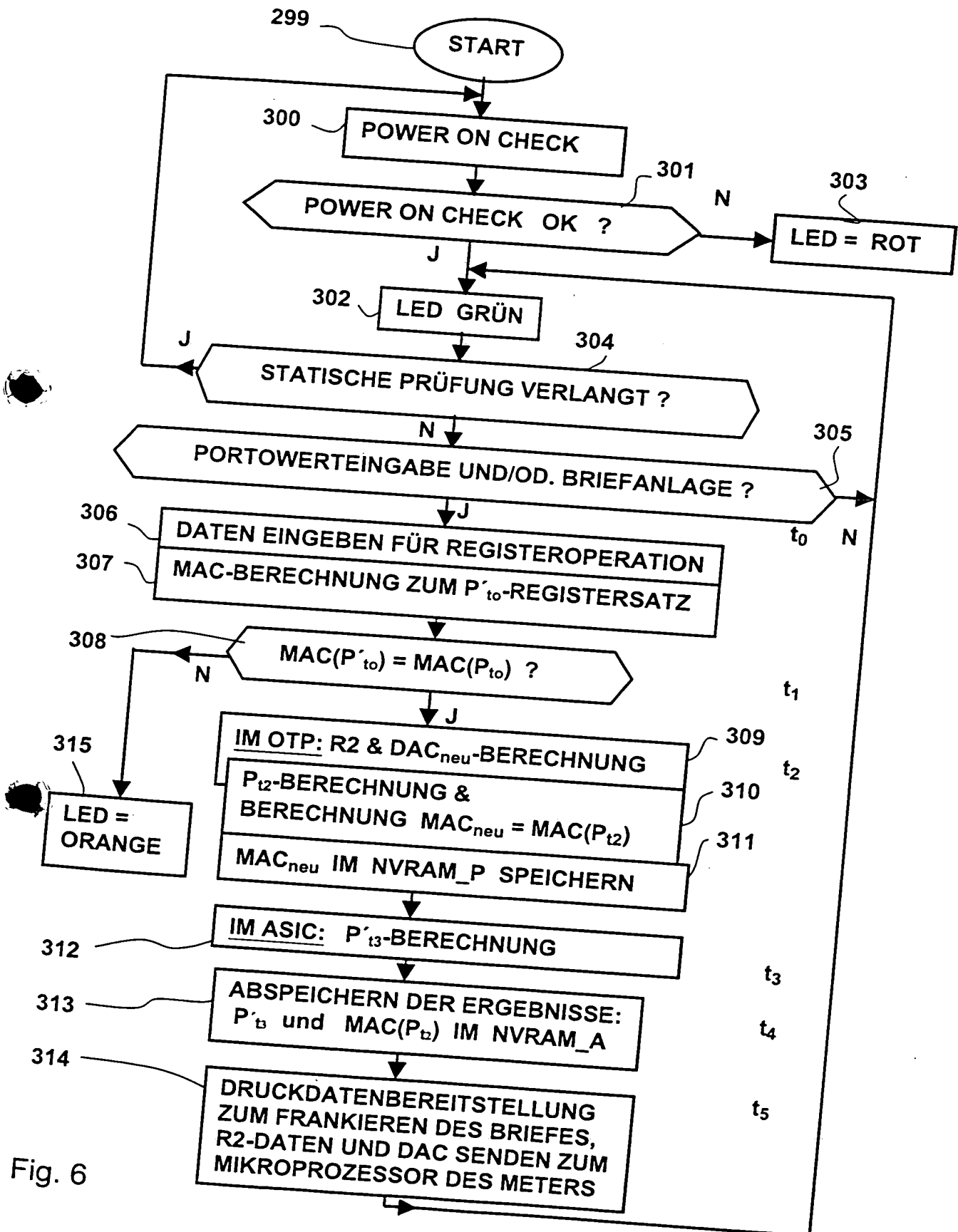


Fig. 6